RPM International Inc.

Employee Data Privacy Policy

Applicable in the United States and Canada

RPM International Inc. ("RPM") and its affiliated companies (separately and collectively the "Company" or "we") are committed to complying with all applicable Data Protection Laws (as defined below). This Employee Data Privacy Policy (the "Policy") a) describes how the Company collects, discloses, uses, or otherwise processes employee Personal Information; b) sets forth the data privacy responsibilities and obligations of Company employees; and c) discloses the data privacy rights afforded to employees under certain Data Protection Laws. This Policy applies to current and former (full-time or part-time) employees, workers, contractors, and agents of any Company (individually referred to as "you").

Data Privacy Principles

We observe the following ten (10) principles related to data privacy in the employment context:

1. **Fairness and Transparency**: We will provide you notice and information concerning how your Personal Information is processed.

2. **Lawful Processing**: We will process your Personal Information in accordance with applicable Data Protection Law.

3. **Purpose Limitation**: We will collect your Personal Information for business purposes and in accordance with the terms and conditions set forth in this and other relevant Company Policies.

4. **Data Minimization**: We will process your Personal Information to the minimal extent necessary to satisfy the purpose for which it was collected.

5. **Accuracy**: We will strive to ensure that your Personal Information is accurate, complete, and up-to-date.

6. **Retention**: We will retain your Personal Information for as long as it is needed to satisfy legal or regulatory obligations, or the Company's business interests.

7. **Security**: We will endeavor to implement and maintain reasonable security measures to protect your Personal Information from unauthorized use, access, or acquisition.

8. **Individual Rights**: We will allow you to exercise the data rights afforded to you under any applicable Data Protection Law.

9. **Data Transfers**: We will implement and maintain safeguards when transferring your Personal Information across international borders.

10. **Accountability**: We will adopt and implement data protection policies and procedures in an effort to ensure your Personal Information is processed in an ethical manner, in compliance with applicable Data Protection Laws and this Policy.

The Personal Information the Company Collects

The Company collects Personal Information about you to perform its business purposes and protect its interests, or as may otherwise be required or permitted by law. Generally, we collect the following types and categories of Personal Information in the employment context:

- **Employee Information:** such as personal and business contact information (e.g., full name, residential address, work address, office location, phone number, and email address); government identifiers (e.g., social security/insurance numbers, driver's license numbers, and passport numbers); financial information (e.g., bank account and salary details); recruitment, pre-employment and employment data (e.g., employment history, educational history, career profiles, attendance records, performance appraisals, and corrective actions); benefits-related information; information concerning retirement, resignation, and other types of termination; working status and employment hours; data in any written agreements between the employee and the Company; information relating to work-related claims, internal investigations and disciplinary proceedings; information held for employment law and health and safety purposes; employee education and engagement history, fitness related information (through voluntary fitness challenges); communications data and other data stored on, or transmitted through, the Company's information resources; photographs and visual images (including video surveillance footage); business travel and expense reporting information; and other similar information.
- **Location Information**: such as when recorded by electronic card access systems, geolocation and tracking mechanism associated with Company vehicles, and the location related to the use of Company's information resources including the management of devices and technology.
- **Technical and Asset Usage Information**: such as information about your use of approved computers, devices, networks, systems, software, telephones, and other information and communications technology that is owned, licensed, or maintained by the Company. For more information about your use of Company assets please see our *Acceptable Use Policy*, which is accessible at https://policies.rpminc.com/legal-compliance-policies/acceptable-use-policy/.
- **Third-Party Information**: we may collect and process Personal Information concerning third parties related to, or otherwise affiliated with, you (e.g., emergency contact information, beneficiary information, and employment references). This information may include special or sensitive categories of data.
- **Special or Sensitive Categories of Data**: As described above, we may collect and process special or sensitive categories of Personal Information that may reveal or identify an

individual's race or ethnic origin, criminal history, religious or philosophical beliefs, sexual orientation, health or medical conditions, or other sensitive data. The Company collects and uses this information in order to comply with the law or its regulatory requirements, assess health and safety conditions, and to further the Company's legitimate business interest, including diversity and inclusion (where permitted and in accordance with applicable law).

- **Biometric Data**: We may collect biometric data for employment, health and safety, security, and administrative purposes. For more information with respect to the Company's collection, use, and processing of biometric data, please see our ***Employee Biometric Data Policy***, which can be accessed at https://policies.rpminc.com/legal-compliance-policies/covid-19-policies/employee-biometric-data-protection-policy/.

The Purpose of the Company's Data Processing

The Company collects and uses Personal Information about, or related to, you and relevant third parties for a broad range of routine legal, business and human resource ("HR") management purposes, including the following:

- **Workforce Planning and Recruitment**, business forecasting, employee assignment planning, budgeting, job advertising, interviewing, and selecting and hiring staff;
- **General Human Resources Management and Administration**, employee career development, performance management, compensation and benefits management and benchmarking, administering payroll and benefit arrangements (including long-term incentive awards and bonus administration), obtaining management and employee satisfaction feedback, managing absences (e.g. sickness, parental leave and other family-related and flexible working policies), health and safety, travel and expense management, general headcount reporting, disaster recovery, emergency response planning and Code of Conduct compliance;
- **Performance of the Company's Business Operations**, executing the Company's day-to-day business activities, allowing employees to work together and collaborate, providing services to customers, and ensuring business continuity;
- **Security Management and Internal Investigations**, ensuring the security of the Company's premises, assets, information, and employees. Individuals who use the Company's information technology ("IT") systems, network, assets, or environment should not expect any privacy related to any information transmitted or stored on the same;
- **Marketing, Advertising and Public Relations**, displaying employees' business contact details (e.g., names or photographs) on the Company's website, or on other social media websites and in other means of communication, such as press releases, newsletters or marketing materials;
- **Complying with Health and Safety Obligations**, including taking the following actions: helping to maintain the health and safety of employees and others in the workforce;

implementing and maintaining emergency and/or exposure management programs concerning hazardous substances; assessing the working capacity of an individual; reintegrating individuals into the workforce (including checking and monitoring fit-for-work status); providing support and care for individuals entitled to benefits in connection with illness or (partial or full) work incapacity; detecting and responding to an incident; managing the employee health file; providing employees with social benefits that depend on the state of an individual's health (e.g., parental leave, sick leave); maintaining proper documentation of accidents and first-aid health care in case of incidents; and responding to pandemics, epidemics, and other health emergencies (including temperature and health screening);

- **Carrying out diversity and equal opportunity monitoring and reporting**, including supportting employees in expressing their individual diversity, ensuring that our workforce is positioned to meet the diverse needs of our consumers, ensuring that talent systems and practices support the full development and advancement of all employees, and generating aggregated level reports and analytics for the Company so that we have a better understanding of our diversity in support of inclusive cultures; and, Legal and Regulatory Compliance, ensuring compliance with health and safety requirements and other legal or fiscal obligations, in connection with litigation or an internal investigation or audit and to ensure compliance with the Company's policies regarding anti-money laundering, bribery, fraud and corruption.

Generally, we processes Personal Information about you because such processing is necessary (i) to establish, manage and terminate the employment relationship , (ii) to satisfy the Company's obligations in connection with an employment contract (e.g., salary disbursement and benefits administration), (iiI) to satisfy the Company's legitimate interests (e.g. to protect the security of the employees, systems, and premises), or (iv) to comply with legal or regulatory requirements. In some circumstances, our data processing is based on consent. We may have multiple reasons to process your Personal Information and the identification of one such reason does not preclude the applicability of any other.

The Company's Disclosure of Personal Information

We may share your Personal Information, across the Company and with external third parties, to satisfy the purposes described above. When appropriate to support our management, administration or business interests, or to comply with legal or regulatory obligations, we may disclose, transfer, or otherwise share your Personal Information with authorized third parties, including (but not limited to) regulatory or law enforcement authorities; government entities; credit professionals; distributors, suppliers, and similar business contacts; outside legal counsel, auditors, and other professional advisors. We may also disclose your Personal Information to third-party service providers, such as the payroll company used to facilitate payment obligations, the administrator of the Company's group pension plan, brokers who are used to obtain insurance and benefits, private medical and dental-care providers, support services, IT support teams, and other types of service providers. However,

we will restrict access to special or sensitive categories of Personal Information to the extent required by applicable Data Protection Law.

We may also share your Personal Information with potential acquirers or investors of the Company. We may share your Personal Information in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of the Company's practice or assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which Personal Information held by the Company, in any form or format, is among the assets transferred.

The Company's Location and Data Transfers; Additional Privacy Rights

RPM International Inc. is headquartered in the United States and has offices and locations in many countries and jurisdictions. We may, in the Company's sole discretion, transfer, process, and retain your Personal Information outside the jurisdiction in which it is collected or where you reside, and in such circumstances, the relevant Personal Information may be available to government authorities under lawful orders and laws applicable in such foreign jurisdictions. Depending on the jurisdiction in which you reside or where the Company conducts its business activities, additional privacy rights and cross-border notice requirements may be applicable. Schedule 1 sets forth those additional privacy rights and requirements.

The Company's Data Retention

We retain your employee records in accordance with industry standards and the Company's internal policies, for as long as needed to satisfy the Company's responsibilities and legal or regulatory obligations, as well as to protect the Company's legal interests and business needs. We will destroy your Personal Information and where necessary any devices and assets that retain or transmit your Personal Information in accordance with industry standards and the Company's internal policies. We may contract with a third-party vendor to perform these data disposal and asset destruction functions on the Company's behalf. For more information, see the RPM International Inc.'s *Records and Information Management Policy*, which is accessible at http://rpmpolicies.rpminc.com/rpm-policies/, the *Email Management Policy*, which is accessible at https://policies.rpminc.com/legal-compliance-policies/email-management/, and the Business Communications Policy, which is accessible at

.

The Company's Use of Artificial Intelligence (AI) Or Similar Technologies

We have developed internal policies and guidance regarding how employees and other personnel should access and use Artificial Intelligence (AI) technologies. When using AI technologies involving Personal Information, we will comply with the data protection principles set forth in this Policy. For example, when purchasing, licensing, or using third party AI technology, we take steps to ensure that all such third-party AI technology (i) satisfies Company principles on responsible use of AI (ii) has adopted appropriate technical and security measures

to safeguard Personal Information, and (iii) any such processing is performed in accordance with and under contractual arrangements designed to protect your Personal Information.

Currently, we do not use AI technologies, such as algorithms that have a sufficient degree of autonomy, derived from your Personal Information to make important or significant decisions about your employment, without human/personal oversight. In other words, all decisions which can affect your status as an employee of the Company are ultimately made by humans.

However, we do use certain AI technologies that allow us to improve efficiency in our daily operations. For instance, we employ and endeavor to implement digital solutions, automation, and advanced technologies that can be used for the following purposes:

- To reduce manual tasks, support our operations, and drive efficiency.
- To improve your well–being and safety at the workplace.
- To comply with internal Company policies and applicable laws, including but not limited to anti– bribery and preventing conflict of interest.
- To protect Company systems, including in the context of cybersecurity or data loss prevention programs.
- To transmit messages and communications through intranet or online chatbots.
- To match your Company profile for career development opportunities.

Where legally required, we will provide you with additional details and information about our use of AI technologies prior to deploying them.

Your Obligation to Safeguard the Personal Information of Others

In the event you have access to the Personal Information of others whether it be customers, business partners, vendors, or other employees, consultants or the like by way of your employment or otherwise in connection with the Company, you shall collect and use such Personal Information in accordance with all applicable Data Protection Laws and Company policies.

If you have access to a sensitive Personal Information like a person's social security number, driver's license number, or other government identifiers, financial information, or the like you shall (i) protect its confidentiality, integrity, and availability, (ii) protect it from any unlawful or unauthorized access, use, or disclosure, including compliance with the RPM *Password Policy*, which can be accessed at https://policies.rpminc.com/data-privacy-policies/password-policy/, and (iii) limit the access and use of such Personal Information to the minimum extent necessary and required to perform an authorized business or legal function.

All new or revised technology, policies, procedures, or activities involving Personal Information must comply with the RPM *DPIA Policy*, which can be found at https://policies.rpminc.com/data-privacy-policies/dpia/dpia-policy/.

If at any time you become aware of, or reasonably suspect, a breach or mishandling of Personal Information, you must immediately notify your supervisor and submit a reportable event at https://rpminc.ethicspointvp.com/custom/rpminc/forms/mgr/form_data.asp?land=en in accordance with the RPM *Reportable Events Policy*, which is accessible at https://policies.rpminc.com/reportable-events-and-hotline-policies/reportable-events/reportable-events-policy/.

Employee Rights and Responsibilities

Depending on the jurisdiction in which you reside, or where the data processing activities are conducted, you may be afforded additional rights or privileges under applicable Data Protection Laws. Schedule 1 sets forth those additional data protection rights or privileges.

To the extent you provide the Company with Personal Information, including Personal Information of a third party, you must (i) ensure, on a continuing basis, the accuracy, reliability, and relevancy of such Personal Information, (ii) collect and provide to the Company such Personal Information in accordance and compliance with all applicable Data Protection Laws, including when applicable, in accordance with all data processing notice and consent requirements, and (iii) inform all third parties whose Personal Information you (or the third party) provide to the Company to facilitate or engage in a personal, non-business-related function, that the Company will collect and retain such Personal Information in accordance with the Company's external *Privacy Policy*, which may be amended from time to time and can be accessed at https://www.rpminc.com/privacy-policy.

Without limiting the foregoing, you must, promptly and without delay, notify the Company (preferably in writing to dataprotection@rpminc.com or your applicable Human Resources or Group Legal Departments) of any amendments that need to be made to your Personal Information, or to Personal Information you provided the Company concerning a third party, to ensure its accuracy, reliability, and relevancy. If you choose not to provide the Company with the Personal Information identified herein, then the Company may not be able to satisfy its own contractual or legal obligations, and in such circumstances, continued employment with the Company may not be permissible, and you acknowledge and agree that the we shall not be held liable for any consequence directly resulting from these circumstances.

If you fail to comply with this Employee Data Privacy Policy, disciplinary action, up to and including termination, may result.

Contact Information

Any questions, concerns, or comments related to how the Company processes your Personal Information, or the rights and privileges described herein, should be directed to your

HR representative, your Group Legal Department or to dataprotection@rpminc.com. For general information about the Company's consumer privacy practices, please visit https://www.rpminc.com/privacy-policy.

Definitions

For purposes of this Policy, the following definitions shall apply:

"**Data Protection Law**" refers to any U.S. and Canadian data protection laws, statutes, and regulations applicable to the Company in the context of the Company's collection, processing, retention, dissemination, disclosure, transfer, disposal, or use of Personal Information.

"**Personal Information**" refers to any information, or a combination of pieces of information, about an individual or that can reasonably identify an individual, and that is subject to, or otherwise afforded protection under, an applicable Data Protection Law.

This policy does not restrict or intend to violate or restrain any personal rights you may be given by law or mandatory legislation in specific jurisdictions, nor does it restrict associates from discussing their wages, hours, or other terms and conditions of employment, or other legally protected activities, including but not limited to under Section 7 of the National Labor Relations Act ("NLRA"). This Policy does not form, in full or in part, any contract of employment or other agreement to provide services, and nothing herein shall be construed to (in any way) terminate, supersede, undermine, or otherwise modify the status of the employment or professional relationship between you and the Company, pursuant to which the Company may terminate the employment or professional relationship at any time, with or without cause, and with or without notice. The Company may amend or update this Policy from time to time and the Company will, when necessary and appropriate, notify you of such amendments and updates.

SCHEDULE 1

JURISDICTION SPECIFIC DATA PROTECTION LAWS

If your Personal Information is subject to, or afforded protection under, any of the following Data Protection Laws, then you are entitled to receive notice of the following:

Canada

Based on certain data protection laws in Canada, employees in some Canadian jurisdictions may have a right to request access and request that the Company update or correct the Personal Information in its custody or control, subject to limited exceptions prescribed by law. Such requests should be directed to your supervisor, an HR representative, your group Legal Department or to dataprotection@rpminc.com. For more information on Canada's provincial and territorial privacy laws and who is responsible for their enforcement, please see the following: https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/provincial-and-territorial-privacy-laws-and-oversight/. If you would like (i) information about the Company's data practices with respect to service providers outside Canada, or how such service providers collect, use, disclose or store Personal Information, or (ii) to file a complaint, or raise concerns about, our data processing activities, please contact the Company at dataprotection@rpminc.com.

United States in General

Without limiting any provisions in the Employee Data Privacy Policy, including this Schedule 1, this Employee Data Privacy Policy, either alone or in conjunction with other Company policies and procedures, satisfies the Company's legal obligation to draft and/or provide notice with regard to how the Company collects, uses, safeguards, disposes, or otherwise processes social security numbers or similar data afforded protection under U.S. state law, including Conn. Gen. Stat. Ann. § 42-471; 201 Mass. Code Regs. §§ 17.01 – 17.04; Mich. CL § 445.84; New Mex. SA 1978, §§ 57-12b-1 – 57¬12b-4; N.Y. Gen. Bus. Law § 399-ddd; and, Tex. Bus. & Com. Code Ann. § 501.0.52.

California

Pursuant to the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 ("CCPA"), California residents are entitled to certain data privacy rights:

- *Right to Know (Specific Pieces of Personal Information).* You have the right to know the specific pieces of your Personal Information that we have collected about you.
- *Right to Know (Categories of Personal Information)*. You have the right to know (i) the categories of Personal Information we have collected from you; (ii) the categories of sources from which the Personal Information is collected; (iii) the categories of your Personal Information we have sold or disclosed for a business purpose; (iv) the categories of third

parties to whom your Personal Information was sold or disclosed for a business purpose; and (v) the business or commercial purpose for collecting or selling your Personal Information.

- *Right to Delete*. You have the right to request that we delete your Personal Information that we have collected and retain.
- *Right to Correct*. You have the right to request that we correct inaccurate Personal Information that we have collected and retain.
- *Nondiscrimination*: The right not to be subject to discrimination for asserting your rights under the CCPA.

Opt Out Rights: Do Not Sell/Share Personal Information. California residents have the right to request that organizations cease "selling" or "sharing" their Personal Information to third parties for profit, monetary or valuable consideration, and under similar circumstances. However, except as otherwise set forth in privacy notices on our external websites available to the general public, the Company does not "sell" or "share" Personal Information regarding our employees to third parties or regarding any person under sixteen (16) years of age, and therefore we do not provide individuals with the ability to opt out of such activities.

Limit Use of Sensitive Personal Information. California residents have the right to request that organizations limit the use of their sensitive Personal Information in certain circumstances. However, the Company does not use or disclose sensitive Personal Information regarding our employees for reasons other than those set forth in the CCPA, and therefore we do not provide individuals with the ability to limit how we use or disclose such sensitive Personal Information.

Submit a Privacy Request. To submit a CCPA privacy request, please contact your supervisor or you may contact us in accordance with the "Contact Information" section above. If you would prefer, you may designate an authorized agent to submit a CCPA privacy request on your behalf. An authorized agent must be registered with the California Secretary of State to conduct business in California.

Privacy Request Verification Process. If you (or your authorized agent) make any request related to your Personal Information under the CCPA, the Company will ascertain your identity (and the identity of the authorized agent, to the extent applicable) to the degree of certainty required or permitted under the law before addressing your request. In particular, the Company will, to the extent required or permitted by law, require you (or your authorized agent) to verify your request via email, request certain contact information or government identifiers, and we will match at least two pieces of such personal information with data that we have previously collected from you before granting you access to, erasing, or correcting, specific pieces or categories of Personal Information, or otherwise responding to your request. We may require written documentation that demonstrates a third party is authorized to serve as your agent for the purposes of submitting the requests set forth herein, unless you have provided the authorized agent with power of attorney pursuant to California Probate Code §§ 4121 to 4130. None of the CCPA's rights are absolute, and such rights are subject to legal and

regulatory exceptions and exemptions. For more information about the CCPA, please see https://oag.ca.gov/privacy/ccpa.**Connecticut**

For purposes of CT ST § 31-48d, the Company engages in "electronic monitoring" and this Employee Data Privacy Policy, and other applicable Company policies, serves as notice of the same. The term "electronic monitoring" means the "collection of information on an employer's premises concerning employees' activities or communications by any means other than direct observation, including the use of a computer, telephone, wire, radio, camera, electromagnetic, photoelectronic or photo-optical systems, but not including the collection of information for security purposes in common areas of the employer's premises which are held out for use by the public, or which is prohibited under state or federal law."

Delaware

For purposes of DE ST TI 19 § 705, the Company monitors or otherwise intercepts the telephone conversations or transmissions, electronic mail or transmissions, or internet access or usage of its employees and of any party accessing the Company's information technology assets, networks, systems, environment, and resources, and the use of the same constitutes consent to the foregoing.

New York

For purposes of NY CIV RTS § 52–c, Company employees are hereby notified that any and all telephone conversations or transmissions, electronic mail or transmissions, or internet access or usage by an employee, by any electronic device or system, including but not limited to the use of a computer, telephone, wire, radio or electromagnetic, photoelectronic or photo-optical systems, that are owned, leased, or operated by the Company may be subject to interception and monitoring at any and all times and by any lawful means.